## REMARKS

Applicants respectfully request entry of the foregoing claim amendments in order to place the application in better form for appeal. Claims 1-6, 8-32, and 34-50 remain in this application, as amended above.

As will be further discussed below, Applicants consider all claims to be in condition for allowance. A notice of appeal was submitted on February 7, 2006. While Applicants are prepared to pursue an appeal of the final rejection, Applicants remain hopeful that this response will demonstrate the patentability of all claims and thereby obviate the need for appeal. At a minimum, Applicants request that the Examiner issue an Advisory Action indicating that the proposed amendments will be entered for purpose of consideration on appeal.

The Examiner rejected Claims 1, 28 and 45 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner refers to two steps relating to the data encrypting key, i.e., "modifying the data encrypting key using location data and encrypting the location-modified data encrypting key using a key encrypting key" (as paraphrased by Examiner). Applicants disagree, and maintains that support for the claim limitations is clearly included in the patent specification.

In particular, the specification describes these steps in connection with the Key Encrypt sub-function 812 shown in Figure 8. According to the specification:

> The Get Key sub-function 806 uses the Key ID 505 to retrieve the appropriate key encrypting key 307a from a key table 306. Then, the Key Encrypt sub-function 812 encrypts the Data Encrypting Key 524 using the Location Value 507 and the key encrypting key 307a. *In a preferred embodiment, the Key Encrypt sub-function 812 first takes the exclusive-OR of the data encrypting key 524 and the Location Value 507, and then encrypts the result using the key encrypting key 307a.*

See p. 26, ln. 24, through p. 27, ln. 1. The cited text provides clear support for the two steps recited in the claim, i.e., the "exclusive-OR" operation of the data encrypting key

with the location value provides the first step, and the encryption of the result provides the second step. This ground of rejection should be withdrawn.

The Examiner also rejected Claims 5, 6, 14, 15, and 46 under 35 U.S.C. § 112, second paragraph, as indefinite. Applicants have amended these claims to address the issues raised by the Examiner.

Specifically, Claim 5 is amended to correct the typographical error identified by the Examiner. Claim 6 is amended to clarify that "said proximity value defines a zone that encompasses said location." Claims 14, 15 and 46 are each amended to recite that the "ability to decrypt" the encrypted digital information is precluded. Applicants consider each of these amended claims to be sufficiently definite to enable persons skilled in the art to understand the invention. No new matter has been added by the proposed amendments. This ground of rejection should also be withdrawn.

The Examiner rejected Claims 1, 8, 11, 13-16, 28, 34, 37-38, and 45-46 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. This rejection is respectfully traversed.

Menezes provides a general text showing the current state of cryptography. The Examiner asserts that Menezes' disclosure of "point-to-point key update using symmetric encryption" would read on "producing an encrypted location-modified data encrypting key produced by encrypting the data encrypting key using a key encrypting key." Applicants respectfully disagree. Menezes discloses a key transport protocol in which a random number selected as the session key is encrypted using a known encryption algorithm and key (see p. 497). This encrypted session key is then communicated to the recipient. Once decrypted, the session key would then be used by the recipient to decrypt communications received from the originator.

Thus, even if the session key of Menezes was construed as providing a data encrypting key, the reference fails to disclose a "location-modified data encrypting key" or any teaching of the desirability of modifying a data encrypting key using location information. The patent application enables a significant improvement in

communication security over Menezes by providing that the recipient can decrypt the message only if (1) it has the appropriate key decrypting key, and (2) it is located at the specific geographic location defined by the location identity data. The Examiner acknowledges that "Menezes does not explicitly teach modifying the data encrypting key using location identity data that defines at least a specific geographic location."

To make up for the deficiency of Menezes, the Examiner now proposes the combination with Laurence et al. The Examiner states that "Laurence et al. teach modifying (encryption) using a specific geographical location (Abstract and col. 23 lines 1-10) in order to prevent reading of the encrypted message by other receivers." Applicants disagree with the Examiner's conclusion that the proposed combination of references suggests or discloses the claims of the patent application.

Laurence et al. is directed to a system for authenticating data transmissions in order to protect against an active attack on a communications system launched by an unauthorized party. According to Laurence et al., an active attack is one in which the unauthorized party injects a fraudulent simulation of a valid communication into the communication path. See col. 2, lns. 13-21. Where the communications system provides transactions for a financial network, for example, the unauthorized communications could result in the receiving station acting improperly, such as by transferring funds to an account accessible to the unauthorized party. Accordingly, the objective of Laurence et al. is to verify the authenticity of the sender of the data transmission.

To accomplish this objective, Laurence et al. discloses the use of the position of the transmitter for authenticating each message that is received by a receiver. See col. 12, lns. 49-54. "Since the transmitting location can be protected physically, it is very unlikely that an unauthorized user will be able to transmit from the proper transmitting location without detection." Col. 12, lns. 58-62. The satellite system that carries the data transmissions can determine the location of the transmitter of each message that is received. See col. 13, lns. 4-7. If proper authentication of the transmitter position does

not occur, the system can determine that an unauthorized message has been received. See col. 13, lns. 9-12.

Laurence et al. discloses several embodiments of the message authentication system. In an exemplary embodiment shown in Fig. 4A, messages are encrypted using the transmitter position element, i.e., the actual location of the antenna of the transmitter. See col. 19, lns. 27-36. As noted by the Examiner, Laurence et al. further discloses that the position information of the intended receiver could also be used to encrypt the message. See col. 23, lns. 1-3. The encrypted message is sent to the satellite, which then determines the location of the transmitter. See col. 19, lns. 37-41. The transmitter location is then appended to the encrypted message and forwarded to the receiver at a second location. See col. 19, lns. 41-44. The receiver then receives the encrypted message with the appended transmitter position data. See col. 19, lns. 45-47. The receiver extracts the transmitter position data from the message and compares it against an authorized transmitter position stored in memory. See col. 19, lns. 47-55. If the extracted position data matches the stored position data, the receiver determines that an authentic message was received and proceeds with decryption of the received message. See col. 19, lns. 55-59.

Unlike the present invention, Laurence et al. does not use location data (either of the transmitter or the receiver) in a key transport protocol. In fact, Laurence et al. contains no disclosure of key transfer whatsoever, and merely refers to the content of the data encrypting key as including location of the transmitter, the sender and/or non-position elements. See, e.g., col. 21, lns. 21-30. Laurence et al. therefore fails to suggest or disclose any use of location information to modify a data encrypting key or the encryption of a location-modified data encrypting key using a key encrypting key. As discussed above, Menezes also fails to suggest or disclose this teaching, and discloses merely a "point-to-point key update" in which a random number selected as the session key is encrypted using a known encryption algorithm and key. Thus, even if combined as proposed, Menezes and Laurence et al. fails to suggest or disclose any

use of location information to modify a data encrypting key or the encryption of a location-modified data encrypting key using a key encrypting key.

The Examiner's burden to present a *prima facie* rejection for obviousness requires: (1) a disclosure or suggestion of every element of the claim in the cited reference or references; (2) a suggestion or motivation, in the references or known to one skilled in the art, to modify or combine the references; and (3) a reasonable expectation of success. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Applicants respectfully submit that the Examiner has failed to satisfy his burden of presenting a prima *facie case* of obviousness due to the absence of any teaching in the art of record of the desirability of using location information to modify a data encrypting key or encrypting a location-modified data encrypting key using a key encrypting key. Moreover, the Examiner has failed to identify any suggestion or motivation to combine the references as proposed. Since Laurence et al. is primarily directed to providing message authentication, and provides no disclosure with respect to key distribution, there would be no motivation for persons skilled in the art to consider the teachings of Laurence et al. to solve a problem relating to secure key distribution and recovery.

In this regard, the Examiner appears to rely entirely upon a hindsight reconstruction of Applicants' claims by selecting statements from the references for support, where the references neither describe nor suggest the proposed combination. This is improper. As the Federal Circuit stated in *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457 (Fed. Cir. 1998):

> This court forbids the use of hindsight in the selection of references that comprise the case of obviousness. See *In re Gorman*, 933 F.2d 982, 986, 18 USPQ2d 1885, 1888 (Fed. Cir. 1991). Lacking a motivation to combine references, the Board did not show a proper prima facie case of obviousness.

The Federal Circuit reinforced this rule in *In re Kotzab*, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000):

> Further, a rejection cannot be predicated on the mere identification in Evans of individual components of claimed limitations. Rather, particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed.

Further guidance is provided by the M.P.E.P. § 2143.01, which states that the prior art must teach the desirability or motivation to reassemble prior art elements in a new combination. The foregoing requirements have not been satisfied with respect to any rejections under § 103(a) traversed herein.

More particularly, with respect to independent Claim 1, the proposed combination of references fails to suggest or disclose a method for controlling access to digital information comprising:

> encrypting said digital information using a data encrypting key;
>
> modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;
>
> encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and
>
> communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location.

Similarly, with respect to independent Claim 28, the proposed combination of references fails to suggest or disclose an apparatus for controlling access to digital information, comprising:

> a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:
>
> encrypting said digital information using a data encrypting key;

modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;

encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and

communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location.

Further, with respect to independent Claim 45, the proposed combination of references fails to suggest or disclose an apparatus for receiving digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

receiving encrypted digital information and an encrypted location-modified data encrypting key;

decrypting said encrypted location-modified data encrypting key using a key encrypting key to obtain a location-modified data encrypting key;

determining a location value that defines a specific geographic location of said apparatus;

extracting a data encrypting key from said location-modified data encrypting key using said location value; and

decrypting said encrypted digital information using said data encrypting key.

The claims dependent upon Claims 1, 28 and 45 are also deemed allowable for the same reasons set forth above. The dependent claims include additional features and limitations not suggested or disclosed by the references. For example, Claim 11 further defines the method of Claim 1 as comprising:

decrypting said encrypted location-modified data encrypting key using a key decrypting key;

using a location value to recover said data encrypting key from said location-modified data encrypting key; and

decrypting said digital information using said data encrypting key.

As discussed above, the proposed combination of Menezes and Laurence et al. fails to suggest or disclose any use of location information to recover an encrypted data encrypting key. Accordingly, these grounds of rejection should be withdrawn.

The Examiner also rejected Claims 2-6, 9-10, 12, 18-19, 29-31, 35-36, 39, and 47 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Murphy. This ground of rejection is also respectfully traversed.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location stored in the receiver/processor for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

As Applicants have noted in previous responses, Murphy does not use location data in the encryption of keys used to protect the underlying digital information. Murphy is directed to a one-to-many communication system in which the same encrypted signals are sent to many users. There is nothing distinctive about the encrypted signals that reflects a transformation using data defining a specific geographic location. In fact, the encrypted signals themselves have no relation to the location information whatsoever. Instead, Murphy uses location information only to determine whether to activate the decryption chip. The SATPS location signal is compared to location information that is previously stored in the receiver, and which has nothing to do with the encrypted signals. Notably, this determination occurs whenever the set-top box

(i.e., receiver) is turned on or after the power supply is interrupted (see col. 8, lines 6-24 and 46-62), i.e., without any consideration of the encrypted signals.

Murphy therefore fails to make up for the deficiencies of Menezes and Laurence et al. Murphy teaches only the use of location as a gate-keeper function in determining whether or not to activate the decryption chip. Murphy does not use location to transform the information or keys being communicated. In fact, Murphy contains no discussion of key selection, generation or usage. Thus, a combination of Menezes, Laurence et al. and Murphy would at most yield a conventional encryption system in which location is used solely to activate the decryption circuitry. The only teaching to use location information to transform the information or decryption keys comes from the present patent application.

This ground of rejection should be withdrawn for the same reasons set forth above with respect to independent Claims 1, 28 and 45. In addition, Murphy further fails to disclose a "shape parameter" as defined in Claim 10. There is no teaching or suggestion to combine Menezes, Laurence et al. and Murphy as proposed, and even if combined, the references fails to suggest or disclose every limitation of the rejected claims.

The Examiner also rejected Claims 21-27, 41-44, and 49-50 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Schneier. This rejection is also respectfully traversed.

Schneier provides a general text showing the current state of cryptography. The Examiner cites Schneier for its disclosure of pseudo-random number generation of a data encrypting key. Respectfully, dependent Claims 21-27, 41-44, and 49-50 relate to the use of key tables to manage the storage of keys, and do not relate to pseudo-random number generation of a data encrypting key. The Examiner fails to establish a *prima facie* case of obviousness insofar as there is no showing that the cited references suggest or disclose all limitations of the rejected claims. Regardless, Schneier fails to make up for the deficiencies of the other references discussed above, and more

specifically, does not use location data to transform the information or keys being communicated. This ground of rejection should therefore be withdrawn.

The Examiner also rejected Claim 19 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and Schneier and further in view of Murphy. This rejection is also respectfully traversed.

The Examiner acknowledges that "none of the references explicitly teach that generating the encryption key comprises using GPS signals to partially seed the pseudo-random number generator." Nevertheless, the Examiner concludes that the use of GPS signals for this purpose would be an obvious design choice. The Examiner provides no evidentiary support for this conclusion. To the extent that the Examiner relies upon Official Notice as a basis for this conclusion, the Examiner is reminded of his obligation under 37 C.F.R. § 1.104(d)(2) that requires the Examiner to provide a suitable affidavit or other evidence to permit contradiction or explanation by Applicants. Without such a showing, it is improper for the Examiner to rely upon such Official Notice as a basis for rejection.

Moreover, there would be no motivation by persons skilled in the art to use GPS signals for such a purpose. To the contrary, the motivation for using GPS signals for this purpose comes directly from the use of location data to transform the information or keys, as taught by the present invention. This ground of rejection should also be withdrawn.

The Examiner also rejected Claims 21-27 and 41-44 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Shibata et al. This rejection is also respectfully traversed.

Shibata et al. discloses a system for communicating encrypted information, and includes a cipher key table in which a plurality of cipher keys are stored. Otherwise, Shibata fails to make up for the deficiencies of the other references discussed above, and more specifically, does not use location data to transform the information or keys being communicated. This ground of rejection should therefore be withdrawn.

The Examiner also rejected Claims 17, 20, 40 and 48 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and Inoue et al. This rejection is also respectfully traversed.

Inoue et al. discloses a packet processing system that eliminates redundant encryption/decryption of message packets passing through intermediate agents between sender and recipient. According to the reference, when relaying encrypted packets of digital information, each node in the relay will decrypt and then re-encrypt the packet. Notably, the Inoue et al. packet processing system does not use location data to encrypt the packet encrypting key. In this respect, Inoue et al. suffers from the same deficiency as Menezes and the other references.

The Examiner also rejected Claims 17, 20, 40 and 48 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Jones et al. This rejection is also respectfully traversed.

Jones et al. disclose an encryption chip that is programmable to process a variety of secret key and public key encryption algorithms. The reference discloses a link encryption application in which encrypted data received at a router between successive links is first decrypted by the chip and then the data is re-encrypted in accordance with the encryption algorithm of the next link. See col. 5, lns. 49-55. As an initial matter, Jones et al. fails to suggest or disclose any use of location information to modify a data encrypting key or the encryption of a location-modified data encrypting key using a key encrypting key, and therefore fails to make up for the deficiencies of Menezes and Laurence et al. discussed above.

Moreover, dependent Claims 17, 20, 40 and 48 include additional features and limitations that are not suggested or disclosed by the proposed combination of references. With respect to Claim 17, Jones et al. fails to disclose a routing step in which a layer of encryption is added to the data encrypting key. Instead, the link encryption application disclosed by Jones et al. strips off the encryption layer before re-encrypting the data. There is no accumulation of encryption layers as disclosed by the

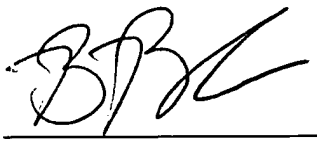
present application. With respect to Claims 20, 40 and 48, Jones et al. fails to disclose use of a location value or location identity data with which to perform the link encryption. This ground of rejection should therefore be withdrawn as well.

To summarize, in view of the absence of any teaching or suggestion of the claim limitations, the Examiner has not met the burden of establishing a *prima facie* case of obviousness. Each of the foregoing grounds of rejection should therefore be withdrawn.

Accordingly, Applicants respectfully submit that Claims 1-6, 8-32, and 34-50 are in condition for allowance and solicit this issuance of a Notice of Allowability. Alternatively, if the Examiner maintains the rejections based on prior art, Applicants respectfully request entry of the foregoing amendments in order to place the application in better condition for appeal. To the extent it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

While the Applicants believe that no fees are due in connection with the filing of this paper, the Commissioner is authorized to charge any shortage in the fees, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,



Date: February 27, 2006

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

**O'MELVENY & MYERS LLP**
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000